IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 10/785,142

Conf. No.: 8153

Appellant: Arbajian

Art Unit: 2139

Filed: 02/24/2004

Examiner: Tabor, Amare F.

Customer No.: 23550

Docket: CHA920040006US1 (IBMC-0104)

Title: SYSTEM AND METHOD FOR PROVIDING DATA SECURITY

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBSTITUTE BRIEF OF APPELLANT

This is an appeal from the Final Rejection (Office Action) dated October 23, 2008, rejecting claims 1-21 and the Examiner's Answer dated March 19, 2009 in which a new ground of rejection was presented. Appellants request that the appeal be maintained. The requisite fees set forth in MPEP 41.20 (b) 1 and 2 were previously submitted on December 18, 2008.

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There is no related appeal or interference.

STATUS OF CLAIMS

As filed, this case included claims 1-21. Claims 1-21 remain pending, stand rejected, and form the basis of this appeal. No claim has been allowed. The rejections of claims 1-21 are being appealed.

STATUS OF AMENDMENTS

No after-final amendment of claims was proposed following the Final Rejection of October 23, 2008.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention, as defined by independent claim 1, is a data security system (page 4, lines 2-3). The data security system includes an implicit clearance system (page 5, lines 16-18), an explicit clearance system (page 5, line 19 through page 6, line 4) and a field level clearance system (page 6, lines 5-11). The data security system further includes a data anonimization system (page 6, line 12-16), wherein each system consists an administrator configuration (page 4, lines 12-16).

A further aspect of the present invention, as defined by claim 12, is a program product stored on a recordable medium for providing data security (page 2, lines 18-19). The program product includes a means for selectively requiring a user to have explicit permission in order to access a set of data (page 4, lines 14-16, Fig. 1, item 16), means for requiring the user to meet any one of a set of implicit conditions in order access the set of data (page 4, lines 14-16, Fig. 1, item 14) and means for limiting access to data records by restricting the user to a predefined

view, wherein the predefined view displays a predetermined set of data fields from the data records (page 6,last line through page 7, line 3; Fig. 1, items 30 and 32). The means for selectively requiring a user to have explicit permission, the means for requiring the user to meet any one of a set of implicit conditions, and the means for limiting access to data records by restricting the user to a predefined view consists of an administrator configuration (page 4, lines 12-16). The program product further provides means for replacing a data element in a data record with a unique identifier in order to create an anonymous data record (page 5, lines 3-6; Fig. 1, item 20).

A further aspect of the present invention, as defined by claim 17, is a method for providing data security (page 3, line 4). The method includes selectively replacing data elements in data records with unique identifiers as the data records are being stored in a data warehouse in order to create anonymous data record (page 5, lines 3-6). The method includes selectively requiring a user to have explicit permission (page 5, line 19 through page 6, line 4) consisting of an administrator configuration (page 4, lines 12-16), in order to access a set of the data records. The method further requires the user to meet any one of a set of implicit conditions (page 5, lines 16-18) consisting of an administrator configuration (page 4, lines 12-16), in order access the set of the data records if explicit clearance is not required. The method limits access to data records by restricting the user to a predefined view consisting of an administrator configuration (page 4, lines 12-16), wherein the predefined view displays a predetermined set of data fields from the data records (page 10, lines 21-25).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-21 are obvious under 35 U.S.C. § 103(a) over O'Flaherty et al. (US 6,275,824), hereinafter "O'Flaherty", in view of Wong et al. (US 6,578,037), hereinafter "Wong"?

2. Whether claims 1 and 17 are directed to statutory subject matter under 35 U.S.C. § 101?

ARGUMENTS

1. Claims 1-21 are not obvious over O'Flaherty in view of Wong.

Independent claims 1, 12 and 17 of Appellants invention all require configuration by an administrator. In claim 1 the following phraseology is used "wherein each system consists of an administrator configuration". In claim 12 the phraseology "wherein the means for selectively requiring a user to have explicit permission, the means for requiring the user to meet any one of a set of implicit conditions, and the means for limiting access to data records by restricting the user to a predefined view consists of an administrator configuration" is used and in claim 17 the phraseology "selectively requiring a user to have explicit permission consisting of an administrator configuration, in order to access a set of the data records, requiring the user to meet any one of a set of implicit conditions consisting of an administrator configuration, in order access the set of the data records if explicit clearance is not required" is used. These claim limitations require that an administrator configure the explicit and implicit or field level clearance systems. A client or consumer is prohibited from configuring such a system.

The Office acknowledges that O'Flaherty fails to teach wherein each system (explicit, implicit and field level) consists of an administrator configuration. The Office cites Wong as disclosing explicit, implicit and field of clearance systems consisting of an administrator configuration. The Office specifically cites FIG. 1 at col. 4, lines 25-47 for support of this assertion. The Office then concludes it would have been obvious to a person having ordinary skill in the art to modify O'Flaherty by incorporating Wong to yield Appellants' invention. Appellants assert that combination of O'Flaherty in view of Wong is not a *prima facia* obviousness type rejection for the reasons below.

The purpose of O'Flaherty is to allow a consumer to specify when and under which circumstances personal information may be retained or shared with or sold to others (col. 5, lines 20-22). The purpose of Wong (col. 5, lines 34-38) is to enable users to independently implement their own policy functions in a manner that reduces or eliminates the need to cooperate with other users. Thus, combining Wong with O'Flaherty, as the Office has done, would render O'Flaherty unworkable. O'Flaherty, as described in col. 4, lines 61, allows a client access and control over data collected from a client. The consumer or client in O'Flaherty can specify data sharing preferences (col. 5, lines 17-18). The combination proposed by the Office would deny the consumer in O'Flaherty the right to specify data sharing preferences, as the administrator would configure access to the data, not the consumer or client. As stated in the MPEP, where a "proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." (MPEP § 2143.01 § V (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984))). Appellants respectfully submit that the modification of O'Flaherty according to the teachings of Wong would render the O'Flaherty invention unsatisfactory for its intended purposes, to wit, to

allow a consumer to specify when and under which circumstances personal information may be retained or shared with or sold to others (col. 5, lines 20-22). In order for the consumer to specify when information is shared, the consumer must be able to configure the system. This is outside the scope of Applellants' claims as the term "consists" is used.

The Office in the Advisory Action of December 4, 2008 has interpreted this argument as asserting that Wong is non-analogous art (See page 2). This interpretation by the Office is not correct and fails to address Appellants' argument detailed above.

In the Examiner's Answer of March 19, 2009, the above argument is characterized as containing contradictory statements. The argument is not self contradictory, the combination proposed by the Office would yield Appellants' invention; however, the combination would modify Flaherty so that it is unsuitable for its intended purpose, to wit, allowing a consumer to specify when and under which circumstances personal information may be retained or shared with or sold to others (col. 5, lines 20-22). The Office denies that this is the purpose of O'Flaherty, yet at col. 4, lines 49-60 it is stated:

> "The limiting access to the data stored in the extended database 106 to access provided by the privacy datatview suite for the purposes of (1)..., (2), and (3) to exclude entire rows (customer records) for opt-out purposes based on consumer opt-outs…"

Thus, the Office is ignoring this explicit purpose of O'Flaherty in the rejection. The combination would make O'Flaherty unsuitable for the purpose of consumer opt-outs.

Therefore, Appellants respectfully request withdrawal of the rejection of claims 1-21.

2. Claims 1 and 17 are directed to statutory subject matter.

Claim 1 of the present invention is directed to a data security system. The system includes an implicit clearance system (Fig. 1, item 14), an explicit clearance system (Fig. 1, item

16), a field level clearance system (Fig. 1, item 18), and a data anonimization system (Fig. 1, item 20). This is a machine that grants, denies, or limits access to data warehouse 22 (page 4, first paragraph). Each system is clearly described in the specification. Appellants submit that claim 1 meets the requirements of statutory subject matter.

Turning to claim 17 a method is recited which limits access to data records by restricting the user to a predefined view. Data elements in data records are selectively replaced with unique identifiers as the data records are being stored in a data warehouse in order to create anonymous data records selectively requiring a user to have explicit permission (Claim 17). Thus, data elements are positively recited as being transformed and claim 17 meets the requirements of 35 U.S.C. § 101. Appellants request withdrawal of the rejection of claims 1 and 17 under 35 U.S.C. § 101.

Appellants respectfully submit that the application is in condition for allowance. Should the Examiner believe that anything further is necessary to place the application in better condition for allowance, the Examiner is requested to contact Appellants' undersigned attorney at the telephone number listed below.

Respectfully submitted,

/Carl F. Ruoff/

Date: April 15, 2009

Carl F. Ruoff
Reg. No. 34,241

Hoffman Warnick LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

CLAIMS APPENDIX

1. A data security system, comprising:

an implicit clearance system;

an explicit clearance system;

a field level clearance system; and

a data anonimization system; wherein each system consists an administrator configuration.

2. The data security system of claim 1, wherein the implicit clearance system comprises a mechanism for setting up a plurality of filters for a set of data, and wherein a user is granted permission to the set of data if the user meets a condition of at least one filter.

3. The data security system of claim 2, wherein the set of data is selected from the group consisting of: a row of data, a data table, and a data field.

4. The data security system of claim 1, wherein the implicit clearance system comprises a table for each filter, wherein each table lists all user ID's that meet the condition of an associated filter.

5. The data security system of claim 1, wherein the explicit clearance system comprises a mechanism for requiring explicit permission to an area of data, and wherein a user is granted permission to the area of data only if explicit permission has been granted.

6. The data security system of claim 5, wherein the area of data is selected from the group consisting of: a row of data, a data table and a data field.

7. The data security system of claim 1, wherein the explicit clearance system comprises:

an explicit areas table that define all areas of data that require explicit clearance; and

a set of ID tables that define those users who have explicit clearance for each of the areas requiring explicit permission.

8. The data security system of claim 1, wherein the field level clearance system controls access to data types by restricting a user to a predefined view, wherein the predefined view displays a predetermined set of data fields.

9. The data security system of claim 8, wherein the field level clearance system includes a set of data type tables that dictates data types available to each of a plurality of users.

10. The data security system of claim 1, wherein the anonimization system provides a mechanism for replacing a data element in a data record with a unique identifier in order to keep the data record anonymous.

11. The data security system of claim 10, wherein the anonimization system includes:

a reference table for each data field that is to be kept anonymous, wherein each reference table includes a list of anonimized data elements and an associated unique identifier; and

a mechanism for generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.

12. A program product stored on a recordable medium for providing data security, the program product comprising:

means for selectively requiring a user to have explicit permission in order to access a set of data;

means for requiring the user to meet any one of a set of implicit conditions in order access the set of data;

means for limiting access to data records by restricting the user to a predefined view, wherein the predefined view displays a predetermined set of data fields from the data records

wherein the means for selectively requiring a user to have explicit permission, the means for requiring the user to meet any one of a set of implicit conditions, and the means for limiting access to data records by restricting the user to a predefined view consists of an administrator configuration; and

means for replacing a data element in a data record with a unique identifier in order to create an anonymous data record.

13. The program product of claim 12, wherein the means for selectively requiring a user to have explicit permission comprises:

means for defining all areas of data that require explicit clearance; and

means for defining those users who have explicit clearance for each of the areas requiring explicit permission.

14. The program product of claim 12, wherein the means for requiring the user to meet any one of a set of implicit conditions comprises means for storing a set of acceptable user ID's for each of the implicit conditions.

15. The program product of claim 12, wherein the means for limiting access to a data record includes means for associating each of a plurality of users with one of the predefined views.

16. The program product of claim 12, wherein the means for replacing a data element in a data record with a unique identifier includes:

reference means for each data field that is to be kept anonymous, wherein said reference means includes a list of anonimized data elements and an associated unique identifier; and

means for generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.

17. A method for providing data security, comprising:

selectively replacing data elements in data records with unique identifiers as the data records are being stored in a data warehouse in order to create anonymous data records;

selectively requiring a user to have explicit permission consisting of an administrator configuration, in order to access a set of the data records;

requiring the user to meet any one of a set of implicit conditions consisting of an administrator configuration, in order access the set of the data records if explicit clearance is not required;

limiting access to data records by restricting the user to a predefined view consisting of an administrator configuration, wherein the predefined view displays a predetermined set of data fields from the data records.

18. The method of claim 17, wherein the step of selectively requiring a user to have explicit permission comprises:

defining all areas of data that require explicit clearance; and

defining those users who have explicit clearance for each of the areas requiring explicit permission.

19. The method of claim 17, wherein the step of requiring the user to meet any one of a set of implicit conditions includes the step of storing a set of acceptable user ID's for each of the implicit conditions.

20. The method of claim 17, wherein the step of limiting access to a data record includes the step of associating each of a plurality of users with one of the predefined views.

21. The method of claim 17, wherein the step of replacing a data element in a data record with a unique identifier includes:

providing a reference table for each data field that is to be kept anonymous, wherein said reference table includes a list of anonimized data elements and an associated unique identifier; and

generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding.